National Infrastructure Protection Center CyberNotes

Issue #2002-11 *June 3, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between May 13 and May 29, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com[1]	Multiple	Office Connect DSL Router 812 1.1.7, 812 1.1.9	A vulnerability exists in PAT (Port Address Translation) which could let an unauthorized remote malicious user obtain access to all ports in the computer behind the router.	No workaround or patch available at time of publishing.	OfficeConnect Port Address Translation Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Bugtraq, May 27, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Amanda[2]	Multiple	Amanda 2.3.0.4	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'amindexd' daemon, which could let a remote malicious user execute arbitrary code as root; and a buffer overflow vulnerability exists in the 'amcheck' utility due to insufficient bounds checking when the command line input is processed, which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: http://download.sourceforge.net/amanda/amanda-2.4.2p2.tar.gz	Amanda Multiple Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
Apache Software Foundation[3]	Unix	Tomcat 3.2.3, 3.2.4	A vulnerability exists when 'source.jsp' is used with a malformed request, which could let a remote malicious user obtain sensitive information including the webroot location.	No workaround or patch available at time of publishing.	Tomcat Source.JSP Malformed Request	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. Proofs of Concept exploits have also been published.
Apache Software Foundation[4]	Unix	Tomcat 3.2.3, 3.2.4	A vulnerability exists in multiple example files that can be requested without any input, which could let a remote malicious user obtain sensitive information including the webroot location.	No workaround or patch available at time of publishing.	Tomcat Example Files Web Root Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Apache Software Foundation[5]	Unix	Tomcat 3.2.3, 3.2.4	A vulnerability exists when the 'realPath.jsp' page is accessed, which could let a remote malicious user obtain sensitive information including the webroot location.	No workaround or patch available at time of publishing.	Tomcat 'RealPath.JSP' Malformed Request	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser. Proof of Concept exploit has also been published.
Apple[6]	Unix	MacOS X 10.1.3	A buffer overflow vulnerability exists in the 'sliplogin' utility, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	MacOS X 'Sliplogin' Buffer Overflow	Medium	Bug discussed in newsgroups and websites.

[2] Bugtraq, May 27, 2002.
[3] Procheckup Security Bulletin, PR02-05, May 29, 2002.
[4] Procheckup Security Bulletin, PR02-07, May 29, 2002.
[5] Procheckup Security Bulletin, PR02-06, May 29, 2002.
[6] SecurityTracker Alert ID 1004317, May 17, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Banner Wheel[7]	Multiple	Banner Wheel 1.0	A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	BannerWheel Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
BlueFace[8]	Windows	Falcon Web Server 2.0.0.1021 SSL Edition, 2.0.0.1021	A vulnerability exists due to a flaw which could let an unauthorized malicious user obtain read access of known password protected files.	No workaround or patch available at time of publishing.	Falcon Web Server File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
bzip2[9]	Unix	bzip2 0.9.5a-d, 0.9.0, 0.9.0a-c, 1.0, 1.0.1	Multiple vulnerabilities exist: a vulnerability exists because files are decompressed insecurely, which could let a file be overwritten without warning; a race condition vulnerability exists that may cause files to decompress with world-readable permissions, which could let a malicious user obtain sensitive information; and a vulnerability exists when a file that is pointed to by a symbolic link is compressed because it inherits the permissions of the symbolic link causing the decompressed file to be world-readable.	Upgrade available at: http://sources.redhat.com/bzip2/index.html#bzip2-latest	bzip2 Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required for the insecure decompression vulnerability and the symbolic link compression vulnerability.
Caldera Interna-tional, Inc.[10]	Unix	OpenServer 5.0.5, 5.0.6	A Denial of Service vulnerability exists in /etc/popper if a malicious user sends an character string of arbitrary length.	Update available at: ftp://stage.caldera.com/pub/security/openserver/CSSA-2002-SCO.20	OpenServer popper Denial of Service	Low	Bug discussed in newsgroups and websites.
Caldera Interna-tional, Inc. [11]	Unix	OpenServer 5.0.5, 5.0.6	A vulnerability exists in the 'SCOAdmin' utility due to predictable naming of temporary files, which could let a malicious user overwrite any file.	Upgrade available at: ftp://stage.caldera.com/pub/security/openserver/CSSA-2002-SCO.22/	OpenServer 'SCOAdmin' Symbolic Link	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[7] Capzlock Security Advisory No. 1, May 20, 2002.
[8] SecurityOffice, May 27, 2002.
[9] FreeBSD Security Advisory, FreeBSD-SA-02:25, May 20, 2002.
[10] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.20, May 22, 2002.
[11] Caldera International, Inc. Security Advisory, CSSA-2002-SCO.22, May 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
CGIScript.net[12]	Unix	csBanner 1.0, csCreate Pro 1.0, csDownload 1.0, csFAQ 1.0, csFiler 1.0, csFileshare 1.0, csGrid 1.0, csIncludes 1.0, csMailto, csNews 1.0, csNews Professional 1.0, csRandom Text 1.0, csUpload 1.0	A vulnerability exists in numerous scripts because they display "debug" data on errors including server paths, form input, and environment values, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CGIScript.net Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco Systems[13]	Multiple	CBOS 2.3.9, 2.3.8, 2.3.7.002, 2.3.7, 2.3.5.015, 2.3.5, 2.3.2, 2.2.1a, 2.2.1, 2.2.0, 2.1.0a, 2.1.0, 2.0.1, 2.3 .053, 2.3, 2.4.1, 2.4.2b, 2.4.2ap, 2.4.2, 2.4.3, 2.4.4	Three remote Denial of Service vulnerabilities exist when a large packet is sent to the Dynamic Host Configuration Protocol (DHCP) port, when a large packet is sent to the Telnet port, and the TCP/IP stack will consume all memory while processing received packets if the CPE processes a high number of overly large packets.	Upgrade available at: http://www.cisco.com	Cisco Broadband Operating System Remote Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[14]	Multiple	Catalyst 4000 5.5.5, 6.3.5, 7.1.2	A vulnerability exists because the switch may not learn the MAC of a connected system until multiple packets have been sent to a host which will cause unicast traffic between the two systems to be broadcast to all systems connected to the switch.	No workaround or patch available at time of publishing.	Catalyst Unicast Traffic Broadcast	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[12] Bugtraq, May 17, 2002.
[13] Cisco Security Advisory, May 23, 2002.
[14] Bugtraq, May 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[15]	Multiple	VoIP Phone CP-7910 3.0-3.2, CP-7940 3.0-3.2, CP-7960 3.0-3.2	Several vulnerabilities exist: multiple Denial of Service vulnerabilities exist using widely available, well-known DoS programs if a malicious user can successfully transmit packets to the IP Telephone; a vulnerability exists when a request is placed to the /PortInformation script with a port ID, which could let a malicious user obtain a dump of the contents of the phone memory; and a vulnerability exists because a default administrative password is hard coded, which could let a malicious user obtain unauthorized access and change configuration information.	Upgrade for the Denial of Service vulnerabilities available at: http://www.cisco.com/tac	VoIP Phone Stream Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information and unauthorized access can be obtained)	Bug discussed in newsgroups and websites. Denial of Service and memory dump vulnerabilities can be exploited via a web browser. There is no exploit code required for the default password vulnerability.
Cisco Systems[16]	Multiple	IOS 11.0 (22a), (18), IOS 11.1 (24a), IOS 11.3 (11b), IOS 12.0 (3)	A Denial of Service vulnerability exists when a malicious user sends a large amount of spoofed ICMP redirect messages.	**Workaround:** Filter inbound ICMP redirect messages or update your IOS to either a not vulnerable release or a fixed version when these become available.	IOS ICMP Redirect Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Compaq Computer Corporation[17]	Multiple	Integrated Administrator firmware 1.0, 1.10	A vulnerability exists in the Integrated Administrator when a user has Telnet, Secure Shell, or console access to the system, which could let an unauthorized malicious user obtain administrative access.	Upgrade available at: http://www.compaq.com/support/files/server/us/download/14569.html	Integrated Administrator Firmware Unauthorized Access	**High**	Bug discussed in newsgroups and websites.
CVS[18]	Multiple	CVS 1.11	A buffer overflow vulnerability exists because the 'rcs.c' file contains an off-by-one error, which could let a malicious user execute arbitrary code.	Upgrade available at: http://ccvs.cvshome.org/servlets/ProjectDownloadList?action=download&dlID=115	CVS Daemon RCS Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Data Wizard[19]	Windows 95/98/NT 4.0/2000	FtpXQ 2.5	A buffer overflow vulnerability exists when an overly long "make directory" request is provided, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	FtpXQ Buffer Overflow	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[15] Cisco Security Advisory, May 22, 2002.
[16] Securiteam, May 21, 2002.
[17] Compaq Security Bulletin, SSRT2179, May 21, 2002.
[18] DER ADV #8, May 25, 2002.
[19] Securiteam, May 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Deerfield.com[20]	Windows NT	WebSite Pro 3.1.11.0	A vulnerability exists due to the way file requests are handled that contains 8.3 short filenames, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.deerfield.com/download/website/	WebSite Pro Filename Request	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
ECS[21]	Multiple	K7S5A(L) V.02/02/06	A vulnerability exists in the firmware distributed with K7S5A boards, which may allow a malicious user access to the boot menu.	No workaround or patch available at time of publishing.	K7S5A Boot Menu Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Eric Raymond[22, 23]	Unix	Fetchmail 5.8.16, 5.8.17, 5.9.1-5.9.9	A buffer overflow vulnerability exists because stack memory space does not check whether the number of e-mails the server claimed was too high, which could let a malicious server write data outside of the array bounds.	**Eric Raymond:** http://tuxedo.org/~esr/fetchmail/fetchmail-5.9.10.tar.gz **RedHat:** ftp://updates.redhat.com/ **Mandrake Linux:** ftp://ftp.rpmfind.net/linux/D/Mandrake/updates/	Fetchmail Message Count Buffer Overflow CVE Name: CAN-2002-0146	Medium	Bug discussed in newsgroups and websites.
Ethereal[24]	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	Ethereal 0.9.3 & prior	Multiple vulnerabilities exist: a Denial of Service vulnerability exists when a malicious user transmits a specially constructed SMB packet across the network; a buffer overflow vulnerability exists in the X11 dissector when keysyms are processed, which could let a malicious user execute arbitrary code; a vulnerability exists in the GIOP dissector mechanism when a specially constructed packet is sent, which could cause an exhaustion of available memory; and a vulnerability exists in the DNS dissector routine when a maliciously constructed DNS query is transmitted across the network, which could let a remote malicious user prevent Ethereal from functioning.	Upgrade available at: http://www.ethereal.com/distribution/ethereal-0.9.4.tar.gz	Ethereal Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
FileZilla[25]	Multiple	FileZilla Server 0.7.0	A Directory Traversal vulnerability exists when a relative path reference is submitted in a FTP command, which could let a malicious user obtain sensitive information.	Upgrade available at: http://prdownloads.sourceforge.net/filezilla/FileZilla_Server_0_7_1.exe	FileZilla Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[20] Securiteam, May 21, 2002.
[21] SecurityFocus, May 28, 2002.
[22] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:047-10, May 20, 2002.
[23] Mandrake Linux Security Update Advisory, MDKSA-2002:036, May 28, 2002.
[24] Security Advisory, enpa-sa-00004, May 19, 2002.
[25] Bugtraq, May 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FreeBSD[26]	Unix	FreeBSD 4.4, 4.5	A vulnerability exists because the k5su utility does not sufficiently validate user group membership if a user has successfully authenticated, which could let a malicious user obtain superuser privileges if the root account password is known.	**Workaround:** k5su may be disabled by removing the setuid bit from the utility. k5su is installed with the krb5 distribution and the utility is now disabled by default in the current version of FreeBSD-STABLE.	FreeBSD k5su Utility Membership Validation	Medium/ **High** **(High if root access is obtained)**	Bug discussed in newsgroups and websites.
FreeBSD[27]	Unix	FreeBSD 4.3-4.5	A vulnerability exists because the current implementation of the setting 'kern.ps_showallprocs=0' fails to protect system processing information, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	FreeBSD Process Information Bypass	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
FreeBSD[28]	Unix	FreeBSD 4.5 RELEASE	A remote Denial of Service vulnerability exists due to an error in the implementation of the accept filters feature.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:26/accept.patch	FreeBSD Accept Filter Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
FreeBSD[29]	Unix	FreeBSD 4.5 STABLE, RELEASE	A vulnerability exists in the 'rc' startup script when X Windows lock files are removed, which could let a malicious user delete arbitrary files.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:27/rc.patch	FreeBSD 'rc' Script Directory Deletion	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Gafware[30]	Windows	CFXImage 1.6.4, 1.6.6	A Directory Traversal vulnerability exists in the 'showtemp.cfm' program due to improper input filtering, which could let a malicious user obtain sensitive information.	Contact the vendor for patch.	CFXImage 'Show Temp.cfm' File Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
GNU[31]	Unix	Mailman 2.0-2.0.10	A Cross-Site Scripting vulnerability exists in the login page, which could let a malicious user execute arbitrary HTML and script code.	**GNU:** http://prdownloads.sourceforge.net/mailman/mailman-2.0.11.tgz **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Mailman Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites.
GNU[32]	Unix	Mailman 2.0.1-2.0.10	A vulnerability exists because HTML tags are not properly filtered from the HTML list archive index, which could let a remote malicious user execute arbitrary HTML and script code.	**GNU:** http://prdownloads.sourceforge.net/mailman/mailman-2.0.11.tgz **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Mailman Pipermail HTML Injection	**High**	Bug discussed in newsgroups and websites.

[26] FreeBSD Security Advisory, FreeBSD-SA-02:24, May 20, 2002.
[27] Bugtraq, May 18, 2002.
[28] FreeBSD Security Advisory, FreeBSD-SA-02:26, May 29, 2002.
[29] FreeBSD Security Advisory, FreeBSD-SA-02:27, May 29, 2002.
[30] Procheckup Security Bulletin, PR02-12, May 29, 2002.
[31] Conectiva Linux Security Announcement, CLA-2002:489, May 24, 2002.
[32] Conectiva Linux Security Announcement, CLA-2002:489, May 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GNU[33] ***Vendors release patches***[34, 35]	**Unix**	**Fileutils 4.0, 4.1, 4.1.6**	**A race condition vulnerability exists in various utilities, which could let a malicious user delete the whole filesystem.** ***Vendors release patches.***	**Patch available for 4.1.6 at:** **http://mail.gnu.org/pipermail/bug-fileutils/2002-March/002440.html** ***Caldera:*** ftp://ftp.caldera.com/pub/updates/OpenLinux/ ***Mandrake:*** http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-031.php?dis=8.1	**Fileutils Race Condition**	**Medium**	**Bug discussed in newsgroups and websites.**
GR Security[36]	Unix	GRSecurity Kernel Patch 1.9.4	A vulnerability exists which could let a malicious user with root access overwrite the memory content even though protection that should forbid this has been implemented in a security patch.	No workaround or patch available at time of publishing.	GRSecurity Linux Kernel Memory Protection	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Harald Hoyer[37]	Unix	Autorun 2.7	A vulnerability exists when a filename is specified to the –c option as an argument, which could let a malicious user view restricted files.	A newer version of the affected product will be included in later releases of Xandros Linux.	Autorun Arbitrary File Read	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hosting Controller[38]	Windows NT 4.0/2000	Hosting Controller 1.1, 1.3, 1.4, 14.b, 1.4.1	Several vulnerabilities exist: a Directory Traversal vulnerability exists because the 'DSNManager' script insufficiently filters sequences from URL parameters, which could let a malicious user obtain sensitive information; and a vulnerability exists in the Import Root Directory (imp_rootdir.asp) script due to inadequate authentication, which could let a malicious user manipulate URL parameters to change the root directory to another arbitrary directory on the system.	No workaround or patch available at time of publishing.	Hosting Controller 'DSNManager' Directory Traversal & Import Root	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Hosting Controller[39]	Windows NT 4.0/2000	Hosting Controller 1.1, 1.3, 1.4, 1.4b, 1.4.1	A vulnerability exists in the 'browse.asp' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Hosting Controller 'Browse.ASP' File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[33] Securiteam, March 15, 2002.

[34] Caldera International, Inc. Security Advisory, CSSA-2002-018.1, May 13, 2002.

[35] Mandrake Linux Security Update Advisory, MDKSA-2002:031, May 16, 2002.

[36] Securiteam, May 18, 2002.

[37] SecurityFocus, May 29, 2002.

[38] Bugtraq, May 17, 2002.

[39] Bugtraq, May 19, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hosting Controller[40]	Windows NT 4.0/2000	Hosting Controller 1.1, 1.3, 1.4, 1.4b, 1.4.1	A vulnerability exists in the default account 'AdvWebadmin' because it is installed with a known password, which could let a remote malicious user obtain administrative access.	**Workaround:** Change the password for the default account or remove the account entirely.	Hosting Controller Default Administrative Account	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
IBM[41]	Unix	DB2 Universal Database for AIX 6.0, 6.1, 7.0-7.2, DB2 Universal Database for HP-UX 6.0, 6.1, 7.0-7.2, DB2 Universal Database for Linux 6.0, 6.1, 7.0-7.2, DB2 Universal Database for Solaris 6.0, 6.1, 7.0-7.2	A buffer overflow vulnerability exists in the 'db2ckpw' utility when a username value greater than eight characters is supplied, which could let a malicious user obtain root privileges.	Hotfix available at: ftp://ftp.software.ibm.com/ps/products/db2/fixes/english-us/	DB2 'db2ckpw' Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
IDS[42]	Multiple	IDS (Image Display System) 0.8.1	A Directory Traversal vulnerability exists when a request for a directory and album name is sent that contains numerous arbitrary character sequences, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Image Display System Directory Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
IPSwitch[43]	Windows NT 4.0/2000, XP	IMail 5.0, 5.0.5-5.0.8, 6.0-6.0.6, 6.1-6.4, 7.0.1-7.0.7, 7.1	A buffer overflow vulnerability exists in the LDAP component, which could let a remote malicious user execute arbitrary code.	Hotfix available at: ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/IM710HF1.exe *Note: Users must be running IMail 7.1 to apply the hotfix.*	IMail Server LDAP Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[40] Bugtraq, May 19, 2002.
[41] IBM Security Advisory, MSS-OAR-E01-2002:318.1, May 24, 2002.
[42] Bugtraq, May 28, 2002.
[43] Foundstone Advisory, FS-052002-21-IPIM, May 20, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IRSSI[44]	Unix	IRSSI 0.8.4	A vulnerability exists because the source code to IRSSI was altered to include a backdoor, which allows a remote malicious user from the IP address 204.120.36.206 to execute arbitrary commands on the host. The source code was Trojaned between the beginning of April and end of May. Downloads of the source code during this time likely contain the Trojan code.	Upgrade available at: http://real.irssi.org/files/irssi-0.8.4a.tar.gz	IRSSI Trojaned Configure File Arbitrary Access	**High**	Bug discussed in newsgroups and websites.
Kismet Project[45]	Unix	Kismet 2.2, 2.2.1	A vulnerability exists when maliciously formatted commands are sent via the SayText() function, which could let a remote malicious user execute arbitrary commands.	Update available at: http://www.kismetwireless.net/code/kismet-2.2.2.tar.gz	Kismet Remote Command Execution	**High**	Bug discussed in newsgroups and websites.
LocalWEB 2000[46]	Windows 98/NT 4.0/2000	LocalWEB 2000 2.1 .0 Standard Version	A vulnerability exists in the protection component, which could let a malicious user bypass password protection and obtain unauthorized access to protected files/folders on the webserver.	No workaround or patch available at time of publishing.	LocalWEB File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Macro-media, Inc.[47]	Windows NT 4.0/2000, Unix	JRun 3.0, 3.1	A buffer overflow vulnerability exists in the ISAPI filter/application when certain HTTP fields are processed, which could let a remote malicious user execute arbitrary code with SYSTEM privileges.	Patch available at: http://www.macromedia.com/v1/Handlers/index.cfm?ID=22273&Method=Full#download Upgrade available at: http://www.macromedia.com/software/jrun/	JRun Header Field Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Matu[48]	Windows 95/98	Matu FTP 1.13	A buffer overflow vulnerability exists which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Matu FTP Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[44] Bugtraq, May 25, 2002.
[45] Bugtraq, May 29, 2002.
[46] Bugtraq, May 24, 2002.
[47] NGSSoftware Insight Security Research Advisory, NISR29052002, May 29, 2002.
[48] Bugtraq, May 22, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
McNews[49]	Multiple	McNews 1.0-1.2	Multiple vulnerabilities exist: a vulnerability exists due to insufficient filtering of URL parameters, which could let a remote malicious user obtain sensitive information; a vulnerability exists because information in the cookie-based authentication credentials is not properly validated, which could let a remote malicious user obtain unauthorized access; a path disclosure vulnerability exists when a malformed web request is made, which could let a malicious user obtain sensitive information; and a vulnerability exists because script code is not properly sanitized from form fields, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	mcNews File Disclosure	Medium/ **High** **(High is arbitrary code can be executed)**	Bug discussed in newsgroups and websites. URL parameters and path disclosure vulnerabilities can be exploited via a web browser. There is no exploit code required for the cookie-based authentication vulnerability.
Meteor Soft[50]	Windows 98/ME	Meteor FTP 1.2b	Several Denial of Service vulnerabilities exists when a malicious user issues multiple arbitrary commands to the server.	No workaround or patch available at time of publishing.	Meteor FTP Multiple Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites.
Microsoft[51]	Windows 2000	Windows 2000 Advanced Server, 2000 Advanced Server SP1&2, Windows 2000 Datacenter Server, 2000 Datacenter Server SP1&2, 2000 Server, 2000 Server SP1&2	A Denial of Service vulnerability exists for querying Active Directory servers using Kerberos V authentication via GSS-A when a specially crafted Active Directory page search query is issued.	No workaround or patch available at time of publishing.	Microsoft Active Directory Denial of Service	Low	Bug discussed in newsgroups and websites.

[49] SecurityFocus, May 20, 2002.
[50] Securiteam, May 28, 2002.
[51] Bugtraq, May 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[52]	Windows 2000	Exchange Server 2000, 2000 SP1&2,	A remote Denial of Service vulnerability exist due to the way malformed RFC-defined mail attributes are handled.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-025.asp	Exchange 2000 Malformed Mail Attribute Remote Denial of Service CVE Name: CAN-2002-0368	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[53]	Windows 95/98/ME/ NT 4.0/2000	Excel 2002	A vulnerability exists because XML stylesheets that contain script can be included with XML documents, which could let a malicious user execute arbitrary embedded script code.	No workaround or patch available at time of publishing.	Excel 2002 XML Stylesheet Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
Microsoft[54]	Windows	MSDE 1.0, SQL Server 2000 Desktop Engine	A vulnerability exists because a null administrative password is set by default, which could let a remote malicious user obtain administrative access. ***Note: A worm is currently propagating due to default null passwords.***	Microsoft has released security recommendations for administrators of SQL server and related products located at: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q322336	MSDE/SQL Server Null Password	**High**	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Microsoft[55]	Windows 95/98/ME/ NT 4.0/2000, XP	MSN Messenger Service 1.0, 2.0, 2.2, 3.0, 3.6, 4.0, 4.5, 4.6	A remote Denial of Service vulnerability exists when a malicious user sends a malformed invite request.	No workaround or patch available at time of publishing.	MSN Messenger Malformed Invite Request Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[52] Microsoft Security Bulletin, MS02-025, May 29, 2002.
[53] Georgi Guninski Security Advisory #55, May 24, 2002.
[54] NTBugtraq, May 23, 2002.
[55] Bugtraq, May 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[56] ***Microsoft releases patch***[57]	**Windows NT 4.0/2000**	**Windows NT Workstation 4.0, 4.0SP1-6a; Terminal Server 4.0, 4.0SP1-6a; Server 4.0, 4.0SP1-6a; Enterprise Server 4.0, 4.0SP1-6a; 2000 Terminal Services 0.0, 0.0SP1-2; 2000 Server 0.0, 0.0SP1-2; 2000 Professional 0.0, 0.0SP1-2; 2000 Datacenter Server 0.0, 0.0SP1-2; 2000 Advanced Server 0.0, 0.0SP1-2**	**A vulnerability exists in the debugging subsystem, which could let a malicious user execute arbitrary code with SYSTEM privileges.**	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-024.asp**	**Windows 2000/NT 4.0 Privilege Elevation** **CVE Name: CAN-2002-0367**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
MIT[58]	Unix	PGP Public Key Server 0.9.2, 0.9.4	A buffer overflow vulnerability exists because long search strings are not handled properly which could let a remote malicious user overwrite stack variables, including the return address.	No workaround or patch available at time of publishing.	PGP Public Key Server Remote Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published
Netscape[59]	Multiple	Netscape Enterprise Server for NetWare 4/5 5.0	A vulnerability exists because several sample files reveal system and path information, which could let a remote malicious user obtain sensitive information including the webroot location.	Temporary Workaround (Procheckup Ltd): Delete all default example programs if not needed.	Netscape Enterprise Web Server for Netware Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploits have been published.

[56] NTBugtraq, March 14, 2002.
[57] Microsoft Security Bulletin, MS02-024, May 22, 2002
[58] Bugtraq, May 24, 2002.
[59] Procheckup Security Bulletin, PR02-1, May 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetScreen[60]	Multiple	ScreenOS 3.0.0, 3.0.0 r1-r4, 2.8.0r1, 2.5r6, 2.5 r1&2, 2.5, 2.6.1, 2.6.1 r1-r5, 2.7.1, 2.7.1 r1-r3, 2.10 r3&4, 3.0.1 r1	A vulnerability exists when an overly long username is sent to the web interface, which could let a remote malicious user cause the device to reboot.	Upgrade available at: http://www.netscreen.com/support/updates.html	ScreenOS Remote Reboot	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
New Atlanta[61]	Windows NT 4.0/2000	ServletExec/ISAPI 4.1	Multiple vulnerabilities exist: a vulnerability exists in the ServletExec/ISAPI when a specially formatted request is sent without a trailing filename, which could let a malicious user learn the physical path of webroot; a file disclosure vulnerability exists in the ServletExec/ISAPI when a request is sent that contains URL encoded directory traversal sequences, which could let a malicious user obtain sensitive information; and a Denial of Service vulnerability exists when a malicious user sends an overly long request via a request for a .JSP file.	There is a workaround for the physical path disclosure bug located at: http://www.newatlanta.com/products/servletexec/self_help/faq_list.jsp The other issues are fixed in Patch #9 available at: ftp://ftp.newatlanta.com/public/4_1/patches/	NewAtlanta Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. Vulnerabilities can be exploited via a web browser.
NullSoft[62]	Windows 95/98/ME/ NT 4.0/2000	Winamp 2.80	A vulnerability exists because authentication credentials for streaming content are stored in plaintext, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Winamp Plaintext Authentication	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
OpenBB[63]	Multiple	OpenBB 1.0.0 RC3	A vulnerability exists because HTML tags are not adequately replaced with BBCodes, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	OpenBB BBCode HTML Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
OpenBB[64]	Multiple	OpenBB 1.0.0 RC1-RC3	A vulnerability exists which could let an unauthorized malicious user obtain administrative access to forums.	No workaround or patch available at time of publishing.	OpenBB Unauthorized Access	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[60] Securiteam, May 27, 2002.
[61] Westpoint Security Advisory, wp-02-0006, May 22, 2002.
[62] Securiteam, May 21, 2002.
[63] SecurityFocus, May 24, 2002.
[64] SecurityFocus, May 24, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenBB[65]	Multiple	OpenBB 1.0.0 RC3	A Cross-Site Scripting vulnerability exists which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	OpenBB Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
OpenBSD[66]	Unix	OpenBSD 3.1	A vulnerability exists on systems using YP with netgroups in the password database because SSHD does ACL checks for the requested user name but uses the password database entry of a different user, which could let a malicious user obtain unauthorized access.	Patch available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/004_sshbsdauth.patch	OpenBSD SSHD Authentication	Medium	Bug discussed in newsgroups and websites.
Opera Software[67]	Windows 95/98/ME/ NT 4.0/2000, XP	Opera Web Browser 6.0.1 win32, 6.0.2 win32	A vulnerability exists because it is possible to bypass the file element's confirmation dialog, which could let a malicious user obtain arbitrary files from client systems.	Upgrade available at: http://www.opera.com/download/	Opera Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Phorum[68]	Multiple	Phorum 3.3.2 a, 3.3.2	A Cross-Site Scripting vulnerability exists in the 'header.php' and 'footer.php' components because user-supplied values of the 'GLOBALS' parameters are not properly sanitized, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://phorum.org/downloads/phorum-3.3.2b3.tar.gz	Phorum Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Phorum[69]	Unix	Phorum 3.3.2 a	A vulnerability exists in the 'plugin.php,' 'admin.php,' and 'del.php' files, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://phorum.org/downloads/phorum-3.3.2b3.tar.gz	Phorum Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
phpBB Group[70]	Multiple	phpBB 2.0.0, 2.0 RC1-RC4, 2.0 Beta 1	A vulnerability exists in BBCode image tags when a certain character are used to close the HTML statement that is created when the BBCode is translated, which could let a malicious user execute arbitrary HTML code.	Upgrade available at: http://www.phpbb.com/downloads.php	PHPBB2 Image Tag HTML Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[65] SecurityFocus, May 24, 2002.
[66] Bugtraq, May 27, 2002.
[67] GreyMagic Security Advisory, GM#001-OP, May 27, 2002.
[68] Bugtraq, May 18, 2002.
[69] Bugtraq, May 18, 2002.
[70] Bugtraq, May 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RedHat[71]	Unix	Stronghold 3.0	A vulnerability exists in the 'SWISH' script, which could let a malicious user obtain sensitive information about the location of the web root path.	No workaround or patch available at time of publishing.	Stronghold 'SWISH" Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Sendmail Consortium [72]	Unix	Sendmail 8.9.0-8.9.3, 8.10-8.10.2 8.11-8.11.6 8.12, 8.12 beta5,7,10, 12, 16, 8.12.1-8.12.3	A Denial of Service vulnerability exists when a malicious user acquires an exclusive lock on files that are required for operation.	**Workaround:** Change file permissions on Sendmail related files to prevent unauthorized users from having lock access. Version 8.12.4 of Sendmail will change the existing permissions of Sendmail-specific files to prevent access from unauthorized users.	Sendmail Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sonic WALL[73]	Multiple	SOHO 6.3.0.0	A security vulnerability exists in the block URL feature, which could let a malicious user insert arbitrary JavaScript code into the log file that is later viewed in its HTML format which will be automatically executed.	No workaround or patch available at time of publishing.	SOHO Content Blocking Script Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
SSH Communi-cations Security[74]	Windows, Unix	SSH2 3.0, 3.0.1, SSH2 for Unix 3.1, 3.1.1, SSH2 for Win32 3.1, 3.1.1	A vulnerability exists which could let a remote malicious user bypass the "AllowedAuthentications" specified in the server configuration.	Upgrade available at: ftp://ftp.ssh.com/pub/ssh/ssh-3.1.2.tar.gz	SSH2 Authentication Bypass	Medium	Bug discussed in newsgroups and websites.
Sun Micro-Systems, Inc.[75]	Unix	in.rarpd	Multiple buffer overflow and string format vulnerabilities exist because proper string formatting is not performed when entries are written to syslog, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Solaris In.Rarpd Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
Sun Micro-Systems, Inc.[76]	Unix	Solaris 9ea & prior	A format string vulnerability exists in the 'in.talkd' daemon, which could let a remote malicious user compromise root.	No workaround or patch available at time of publishing.	Solaris in.talkd Remote Root Compromise	**High**	Bug discussed in newsgroups and websites.

[71] Bugtraq, May 21, 2002.
[72] Bugtraq, May 23, 2002.
[73] Securiteam, May 18, 2002.
[74] Bugtraq, May 23, 2002.
[75] DER Adv #7, May 22, 2002.
[76] Next Generation Security Technologies Security Advisory, NGSEC-2002-3, May 23, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[77]	Unix	Answer Book2 1.4-1.4.3	A buffer overflow vulnerability exists in the 'gettransbitmap' cgi due to improper bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AnswerBook2 Gettransbitmap Buffer Overflow CVE Name: CAN-2002-0360	**High**	Bug discussed in newsgroups and websites.
TransSoft[78]	Windows 95/98/NT 4.0/2000	Broker FTP Server 5.0	A Denial of Service vulnerability exists when a malicious user submits multiple malformed "change directory" commands.	No workaround or patch available at time of publishing.	Broker FTP Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Trend Micro[79]	Windows NT 4.0	InterScan VirusWall for Windows NT 3.52	A vulnerability exists because headers from e-mail messages that are passed to the MTA are not preserved, which could let a malicious user spam the host without being traced and send misinformation.	Upgrade available at: http://www.antivirus.com/download/updates.asp	InterScan VirusWall SMTP Header Removal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
ViewCVS[80]	Unix	ViewCVS 0.8-0.9.2	A Cross-Site Scripting vulnerability exists because HTML tags are not filtered from certain URL parameters, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	ViewCVS Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
Virtual Program-ming[81]	Windows 95/98/NT 4.0/2000, XP	VP-ASP 4.0	Multiple vulnerabilities exist: a vulnerability exists if the '/demo400/shopdbtest.asp' test page that is included in the default installation is not removed, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because user-supplied input is not sanitized before being used in a SQL query, which could let a malicious user bypass authentication.	No workaround or patch available at time of publishing.	VP-ASP Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
WoltLab[82]	Unix	Burning Board 1.1.1	A vulnerability exists due to a flaw in the randomization function, which could let an unauthorized malicious user obtain access to another user's account.	No workaround or patch available at time of publishing.	Burning Board Randomization Function	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[77] eSecurityOnline Advisory 5063, May 20, 2002.
[78] Securiteam, May 28, 2002.
[79] Bugtraq, May 24, 2002.
[80] Securiteam, May 19, 2002.
[81] Kowchews Security Advisory, May 27, 2002.
[82] Bugtraq, May 26, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xerox Corporation[83]	Multiple	DocuTech 6110, 6115	Several vulnerabilities exist: a vulnerability exists in the printer portion of the system due to a weak default configuration and a known root password, which could let an malicious user obtain unauthorized access; and a vulnerability exists in the scanner portion of the system because the system is configured with the entire C drive being shared, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	DocuTech Printer & Document Scanner Insecure Default Configuration	Medium	Bug discussed in newsgroups and websites.
Yahoo![84]	Windows 95/98/ME/ NT 4.0/2000, XP	Instant Messenger 5.0	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'Call Center' component, which could let a malicious user execute arbitrary code; and a vulnerability exists because it is possible to use a URL beginning with ymsgr:addview? to point to a web page containing arbitrary script which will be executed by the Yahoo! Instant Messenger.	Upgrade available at: http://download.yahoo.com/dl/installs/ymsgr/ymsgr_1065.exe	Instant Messenger Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
YoungZ Soft[85]	Multiple	Cmail Server 3.30	A buffer overflow vulnerability exists due to improper bounds checking on the USER argument, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	CMailServer Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

[83] Bugtraq, May 17, 2002.
[84] Bugtraq, May 27, 2002.
[85] Bugtraq, May 21, 2002.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between May 17 and May 29, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 20 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 29, 2002	Yahoo-im.txt	Document that describes information regarding the Yahoo! Instant Messenger buffer overflow vulnerability and a "how-to" explaining the technique to use to hijack another IM client.
May 28, 2002	**Ids-inform.pl**	**Perl script which exploits the Image Display System Directory Disclosure vulnerability.**
May 28, 2002	Uw-imap.c	Script which exploits the Imap4 remote Linux vulnerability.
May 28, 2002	War-ftpd-bof.pl	Perl script that exploits the WarFTPd remote buffer overflow vulnerability.
May 28, 2002	Wpoison-dev.tgz	A tool that attempts to find SQL-injection vulnerabilities on a remote web document.
May 25, 2002	**Sendmail-flock-sploit.txt**	**Local exploit for the Sendmail Denial Of Service vulnerability.**
May 24, 2002	Wellenreiter-v13.tar.gz	A GTK/Perl program that makes the discovery and auditing of 802.11b wireless networks much easier.
May 24, 2002	**Xls_sux.xls**	**Exploit for the Excel 2002 XML Stylesheet Arbitrary Code Execution vulnerability.**
May 23, 2002	Boegadt_beta-1.0.tar.gz	A Unix-based library that attempts to make it easy to write buffer overflow exploits.
May 23, 2002	**Freebsdsendmaildos.c**	**Script which exploits the Sendmail Denial Of Service vulnerability.**
May 23, 2002	**Freebsdsendmailpoc.c**	**Script which exploits the Sendmail Denial Of Service vulnerability.**
May 23, 2002	Lcrzoex-4.10-src.tgz	A toolbox for network administrators and network malicious users that contains over 200 functionalities using network library lcrzo. For example, one can use it to sniff, spoof, create clients/servers, create decode and display packets, etc.
May 22, 2002	**Matuftpwin98.pl**	**Perl script which exploits the Matu FTP Server Buffer Overflow vulnerability.**
May 22, 2002	Sql_injection_walkthrough.txt	Document that describes SQL injection attack web applications by submitting raw SQL queries as input.
May 21, 2002	**Cmaileexp.c**	**Script which exploits the CMailServer Buffer Overflow vulnerability.**
May 19, 2002	Ethereal-0.9.4.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
May 19, 2002	Ie.css.txt	Online demonstration exploit for the IE showModalDialog and showModelessDialog vulnerabilities.
May 18, 2002	**Hp-sap_evade.pl**	**Perl script which exploits the FreeBSD Process Information Bypass vulnerability.**
May 18, 2002	**Kmem_mmap.tgz**	**Exploit script for the GRSecurity Linux Kernel Memory Protection vulnerability.**
May 17, 2002	**Show_debug_data.pl**	**Perl script which exploits the CGIScript.net Information Disclosure vulnerability.**

Trends

- **The National Infrastructure Protection Center (NIPC) is monitoring an Internet worm called "Spida," also known as SQLSnake. This worm takes advantage of default settings within Microsoft's SQL Server (MSSQL) when there is a system administrator username of "sa" and no password. Administrators are advised to change all passwords on infected machines, not simply that of the system administrator account, For more information see "Bugs Holes & Patches" and Virus Sections. Also see NIPC Advisory 02-003 located at: http://www.nipc.gov/warnings/advisories/2002/02-003.htm.**
- There has been an increase in the number of scans to port 80 scans, still being caused by Nimda and Code Red.
- There has been an increase in the number of scans to port 1433 lately. The most common use of this port is Microsoft's SQL server. A vulnerability in SQL Server 7.0 and 2000 exists which allows access to the security context of the server. Microsoft released an advisory and a patch for this problem which is available at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-020.asp.
- **The National Infrastructure Protection Center (NIPC) continues to monitor a mass-mailing worm called Klez.h. The NIPC is issuing this alert due to information received from industry partners, combined with the striking number of infections reported in the wild. For more information, see NIPC ALERT 02-002, located at: http://www.nipc.gov/warnings/alerts/2002/02-002.htm.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

HTML_GODWILL.A (Alias: Downloader-X.ldr) (HTMLVirus): This HTML virus exploits a known vulnerability in Internet Explorer 5.5 and Microsoft Outlook, which allows the execution of arbitrary programs by script embedded in a Web page or an HTML-based e-mail message. It uses the system class, com.ms.activeX.ActiveXComponent, as a Java object, calling it using the &ltAPPLET> tag. The com.ms.activeX.ActiveXComponent Java object allows the creation and scripting of arbitrary ActiveX objects, which in this case, is the malware, JAVA_GODWILL.A.

JS/SQLSpida.a.worm (Aliases: Digispid.Worm, JS/SQLSpida.js.a, JScript/SQLSpida.A.Worm, W32/SQLSpider-A, Worm.SQL.Access.20) (JavaScript Worm): This worm has been reported in the wild. It targets Microsoft SQL servers. The worm probes the Internet for SQL servers on port 1433 and compromises those servers using the default SQL administrator account "SA." SQL administrators should take appropriate action to ensure that the "SA" account is not vulnerable. For information on securing your SQL server see: SQL Server w/ Blank SA Password Opens Vulnerability to Worm, located at: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313418. Once a SQL server has been accessed, the worm creates the NT user "sqlagentcmdexec," sets a password on that account, adds the user to the local administrators group and adds the user to the "Domain Admins" group. The worm then writes several files to the compromised server and kicks off the propagation routine.

JS/SQLSpida.b.worm (Aliases: BAT_SQLSPIDA.B, Digispid.B.Worm, JS.Spida.B, JS/SQLSpida.bat.b, JS/SQLSpida.js.b, JS_SQLSPIDA.B, JScript/SQLSpida.Worm) (JavaScript Worm): This worm targets Microsoft SQL servers. It probes the Internet for SQL servers on port 1433 and compromises those servers using the default SQL administrator account "SA." SQL administrators should take appropriate action to ensure that the "SA" account is not vulnerable. For information on securing your SQL server see: SQL Server w/ Blank SA Password Opens Vulnerability to Worm, located at: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313418. Once a SQL server has been accessed, the worm activates the NT user guest, sets a password on that account, adds the user to the local administrators group and adds the user to the "Domain Admins" group. The worm then writes several files to the compromised server and kicks off the propagation routine.

Linux.Simile (Aliases: Win32, Linux}/Simile.D, {Win32, Linux}/Etap.D) (Win32 Virus & Linux Virus): This is a very complex virus that uses entry-point obscuring, metamorphism, and polymorphic decryption. It is the first known polymorphic metamorphic virus to infect under both Windows and Linux systems. The virus contains no destructive payload, but infected files may display messages on certain dates. It is the fourth variant of the Simile family. This variant introduces a new infection mechanism on Intel Linux platforms; infecting 32-bit ELF files (a standard Unix binary format). The virus infects PE files as well as ELFs on both Linux and Win32 systems.

VBS_ANJULIE.J (Visual Basic Script Malware): This Malware has been reported in the wild. It uses Microsoft Outlook to propagate copies of itself via e-mail. It sends itself as an attachment in an e-mail that is sent to all recipients listed in the infected user's address book. It can also send itself via mIRC. It creates an IRC script, "IRC_ANJULIE.J."

VBS/Horty.c@MM (Visual Basic Script Worm): The virus may arrive as an e-mail attachment, "Monica-Bellucci.jpg.vbs" and will send an e-mail using Outlook in the following format:

- Subject: Here you have, ;o)
- Body: "Hi (username).Check This!
- Attachment: Monica-Bellucci.jpg.vbs

It then copies the following infected files to the Windows Directory:

- Monica-Bellucci.jpg.vbs
- run32dll.vbs

VBS/Horty.c@MM also uses an infection counter in : HKLM\SOFTWARE\TaskManager. If counter value is less than 8, the virus e-mails out to all recipients in the Outlook Contact folder in the above format. If the infection counter is equal to 10, the virus deletes *.exe in windows folder and then displays a message.

VBS_LEE.F (Aliases: LEE, I-WORM.LEE, VBS/VBSWG) (Visual Basic Script Virus): This nondestructive, Visual Basic Script virus displays the following text strings:

- "You have been infected by the ShakiraPics Worm."

It propagates copies of itself via Internet Relay Chat (mIRC) and e-mail. It sends out e-mail messages with the following characteristics:

- Subject: Shakira's Pictures
- Message Body: Hi! I have sent the photos via attachment. Have funn...
- Attachment: ShakiraPics.jpg.vbs

VBS_PLEXIS.A (Visual Basic Script Virus): This nondestructive virus infects Microsoft Word and Excel files. It uses Mail Application Programming Interface (MAPI) functions to send e-mail messages containing a copy of "PE_PLEXIS.A" as attachment to all the recipients listed in the infected user's address book.

VBS/Redlof-A (Visual Basic Script Virus): This virus infects HTM, HTML, ASP, PHP, JSP, HTT, and VBS files by appending a VBScript that contain an encrypted copy of the virus code to them. The virus exploits the Microsoft VM ActiveX component vulnerability enabling the virus to be activated by viewing an infected HTML document at a remote site. VBS/Redlof-A will attempt to propagate via e-mail sent by the infected user. This is achieved by infecting blank.htm, the default stationery file for Microsoft Outlook or Outlook Express. This file is commonly found in the folder C:\Program Files\Common Files\Microsoft

Shared\Stationery\ . An appropriate registry entry is edited to ensure that the infected user includes the default stationery file when they compose an e-mail. The registry entries targeted are:

- HKCU\Identities\<DefaultId>\Software\Microsoft\Outlook Express\<OutlookVersion>\Mail\Compose Use Stationery,
- HKCU\Identities\<DefaultId>\Software\Microsoft\Outlook Express\<OutlookVersion>\Mail\Stationery Name,
- HKCU\Identities\<DefaultId>\Software\Microsoft\Outlook Express\<OutlookVersion>\Mail\Wide Stationery Name,
- HKCU\Software\Microsoft\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet Settings\0a0d020000000000c000000000000046\001e0360,
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Outlook Internet Settings\0a0d020000000000c000000000000046\001e0360,
- HKCU\Software\Microsoft\Office\10.0\Common\MailSettings\NewStationery.

An infected VBScript is dropped to the Windows system folder with the name “kernel.dll.” This file is pointed to by the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Kernel32

so that it is executed when Windows is started up. The virus also modifies the registry entries:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\.dll
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\dllfile

so that files with DLL extensions are executed as scripts using wscript.exe. Microsoft has issued a security patch that secures against the VM ActiveX component vulnerability. It is available at http://www.microsoft.com/technet/security/bulletin/MS00-075.asp.

W32/Benjamin-A (Alias: Worm.Kazaa.Benjamin) (Win32 Worm): This worm has been reported in the wild. It exploits the Kazaa file exchange peer to peer network as a means of propagation. When first executed, the worm will display a message box containing the false error message, "Access error #03A:94574: Invalid pointer operation File possibly corrupt." A copy of the worm will then be placed in the Windows system folder and a value named System-Service will be added to the registry at:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run .

This entry will run the worm when Windows is started. A large number of copies of the worm will be placed in the folder, C:\Windows\Temp\Sys32. This folder is registered as the location where Kazaa users have access to download files. The intention is for Kazaa users to unknowingly download the worm. To increase the chances of this occurring the copies of the worm are given names that often correspond with song, film, and computer game titles. The worm will attempt to display a web page from benjamin.xww.de. However, the page that the worm attempts to display has been removed.

W32/Nahata-E (Alias: I-Worm.Nahata) (Win32 Worm): This is an intended worm that tries to spread via e-mail, mIRC, and Pirch. It drops itself into the root folder of drive C:. It drops the file C:\info.vbs. Info.vbs should send the worm to e-mail addresses found in the Outlook address book and overwrite script.ini and events.ini when the computer is restarted. However, it does not work properly. W32/Nahata-E sets the registry entries:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MyID = path to the program
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\COUNT = 20.

Each time the worm is run, it will decrement the COUNT value stored in the registry. When the value reaches 0, the worm will remove the registry entries.

W97M/Hich.a (Word 97 Macro Virus): The virus disables the Word virus protection feature and also disables the esc key. W97M/Hich.a is a parasitic virus. It may use the same subroutine name Document_Close if already present by inserting a call to it's viral routine. The virus then appends the viral routine. If Minute = 1, the virus can delete characters in the contents of the document. If Minute = 26, the virus can delete all contents of the document.

W97M.Sacep.B (Word 97 Macro Virus): This is a Microsoft Word Macro virus that infects Word documents when they are closed. On the 13th of every month, the virus inserts the text "pequitas te amo" into the current document.

WM97/Marker-AK (Word 97 Macro Virus): This is a variant of the WM97/Marker-A Word macro virus. It has no malicious payload and does little more than replicate.

Worm/Brit.E (Internet Worm): This is a slight variation of Worm/BritneyPic, an Internet worm that spreads through e-mail by using addresses it collects in the Windows Address Book, as well as, through mIRC. This new variation arrives as," ILOVELAURAYOU.chm." It adds a copy of itself (ILOVELAURAYOU.chm) in the /windows/ directory. Additionally, it modifies the file "Script.ini" if found.

WORM_ENEMANY.A (Aliases: W32/Enemany.a.intd) (Internet Worm): This non-destructive, non-memory resident mass-mailing worm sends copies of itself via e-mail to all contacts listed in an infected user's Microsoft Outlook address book. When the worm runs, it does the following:

- It sends e-mail to all contacts in the Microsoft Outlook Address Book. It attempts to attach a file to the e-mail, but fails in the attempt. The e-mail message is as follows:
  - Subject: The New Xerox Update for our WinXP
  - Message: Dear, Microsoft WinXP User, here are the last Update from Xerox Security System, please install this file and going to www.microsoft.com and finished this Update too.
- It then copies itself as:
  - C:\Windows\Start Menu\Programs\StartUp\WinUpdate.exe
  - C:\Windows\System\Ati.scr
  - C:\Windows\Xerox-Update.exe

WORM_ENEMANY.B (Aliases: W32/Enemany.b@MM, Win32.Enemany.B) (Internet Worm): This is a mass-mailing worm which sends itself to all contacts in the Microsoft Outlook Address Book. It copies itself as:

- C:\Windows\System\Edonkey.scr
- C:\Windows\Esel_Update.exe

WORM_ENEMANY.C (Alias: WORM_ORUET.A) (Internet Worm): This non-destructive, non-memory resident, mass-mailing worm sends copies of itself via e-mail to all contacts listed in an infected user's Microsoft Outlook address book.

WORM_FRETHEM.A (Alias: W32/Win64.a) (Internet Worm): This UPX-compressed, memory-resident worm propagates via e-mail, sending out messages with the following characteristics:

- Subject: Re: Do your Windows looks like Windows XP? I have found very nice desktop themes!
- Message Body: Hello! Do you like modern design of new Windows XP?! I have found FREE and easy to use desktop themes! You can open attach with web site and samples! Enjoy it!!!
- Attachment: www.freedesktopthemes%random number%.com

This worm gets its recipients from the infected user's Windows Address Book (WAB) and from .DBX files, which are the Microsoft Outlook Express mail archives.

Worm/Lentin.E (Internet Worm): This is an Internet worm that arrives as a Lovers Screen Saver, "love4u.scr." It is a modification of Worm/Lentin (Valentine.scr), an Internet worm that spreads by retrieving e-mail addresses from the Windows Address Book, as well as, from addresses found in cached webpages. It can also spread through the use of MSN Messenger. This variant arrives with the subject line: "Lovers Screen Saver (www.love4u.com)!" If executed, the worm copies itself in the \Recycled\ directory under a random filename (ie. "SXKL.EXE." Additionally, a text file (using the same random characters) is also created in the /windows/ directory. It also modifies the following registry key:

- HKEY_CLASSES_ROOT\exefile\shell\open\command @="\ %1 %*" @="\"c:\recycled\sxkl\" %1 %*"

This modification allows it to run each time another executable file is ran. Running the worm will display a screensaver with a multicolor screensaver message that shakes the screen after it is complete.

WORM_YAHA.D (Internet Worm): This worm drops files on the infected user's system and modifies the registry so that it executes whenever the infected user runs an .EXE file. It does not have a destructive payload.

X97M.Draco (Excel 97 Macro Virus): This is a Microsoft Excel macro virus that inserts its viral code into C:\Program Files\Microsoft Office\Office\Xlstart\Book1.xls. During the month of May, the virus will automatically close the current workbook.

X97M.Ellar.E (Excel 97 Macro Virus): This is a macro virus that infects Microsoft Excel 97 and later workbooks and templates. The viral code is inserted into a macro module named Module1.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2002-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
APStrojan.sl	N/A	CyberNotes-2002-03
Arial	N/A	CyberNotes-2002-08
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Omed.B	**N/A**	**Current Issue**
Backdoor.Palukka	N/A	CyberNotes-2002-01
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
BackDoor-AAB	N/A	CyberNotes-2002-02
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
BDS/Osiris:	N/A	CyberNotes-2002-06
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Dewin	N/A	CyberNotes-2002-08
DlDer	N/A	CyberNotes-2002-01
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	N/A	CyberNotes-2002-08

Trojan	Version	CyberNotes Issue #
Fortnight	N/A	CyberNotes-2002-10
Hacktool.IPStealer	N/A	CyberNotes-2002-02
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
JS/NoClose	**N/A**	**Current Issue**
JS/Seeker-E	N/A	CyberNotes-2002-01
JS_EXCEPTION.GEN	N/A	CyberNotes-2002-01
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
QDel227	N/A	CyberNotes-2002-09
QDel234	**N/A**	**Current Issue**
RCServ	N/A	CyberNotes-2002-10
SecHole.Trojan	N/A	CyberNotes-2002-01
Tr/WiNet	N/A	CyberNotes-2002-10
TR/Zirko	N/A	CyberNotes-2002-10
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/Download-A	N/A	CyberNotes-2002-01
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	**N/A**	**Current Issue**
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Optix-03-C	N/A	CyberNotes-2002-01
Troj/Sub7-21-I	N/A	CyberNotes-2002-01
Troj/WebDL-E	N/A	CyberNotes-2002-01
TROJ_CYN12.B	N/A	CyberNotes-2002-02
TROJ_DANSCHL.A	N/A	CyberNotes-2002-01
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_FRAG.CLI.A	N/A	CyberNotes-2002-02
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
TROJ_SQLSPIDA.B	**N/A**	**Current Issue**
Trojan.Badcon	N/A	CyberNotes-2002-02
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.StartPage	N/A	CyberNotes-2002-02
Trojan.Suffer	N/A	CyberNotes-2002-02
VBS.Gascript	N/A	CyberNotes-2002-04
VBS_CHICK.B	N/A	CyberNotes-2002-07
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06

Trojan	Version	CyberNotes Issue #
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Tendoolf	N/A	CyberNotes-2002-09
WbeCheck	N/A	CyberNotes-2002-09

Backdoor.Omed.B (Aliases: TrojanDownloader.Win32.Smokedown): This is a Trojan horse which downloads a file from the Internet and executes it. At the time of writing, this downloaded file contained two different Backdoor Trojans.

JS/NoClose (Aliases: TROJAN.NOCLOSE, JS.TROJAN.NOCLOSE, HTML.JSCRIPT.NOCLOSE): This Trojan has been reported in the wild. It is a JavaScript Trojan. When an affected website is accessed, the Trojan will minimize Internet Explorer and attempt to access other websites without the user's express permission. These sites either contain advertisements or pornographic material.

QDel234: This is a DOS executable Trojan, which deletes critical system files from the victim machine when run. The Trojan has been manually e-mailed to the target as an attachment to an e-mail in which the sender claims to have hacked your web site. When executed on the victim machine a message is displayed to the user. Once the user presses a key, the following files are deleted from the machine:

- *.ini and *.exe from C:\windows\system
- *.dll and *.exe from C:\windows

The above file paths are hardcoded within the Trojan.

Troj/Momma-B: This is a backdoor Trojan and Denial of Service attack tool. It allows a remote malicious user access to the machine via IRC channels and allows them to carry out Denial of Service attacks on the local network. Troj/Momma-B creates a hidden folder named \INF\internet\ in the Windows folder. It then installs the files command.exe, D3dxfo.dll, icmpfilter.dll, inf.exe, mirc.ini, remote.ini, Rvspsp.dll, and vbejat32.dll along with the legitimate files mswinsck.ocx, and wsminsck.ocx. It also creates the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\InternetExplorer =<Windows folder>\INF\internet\inf.exe

so that the Trojan is run automatically each time Windows is started. When the Trojan runs, it tries to connect to an IRC server and join a specific channel. It then runs in the background as a server process, listening on the IRC channel for commands from a malicious user. When it receives a command, it will perform the specified action, such as executing a malicious IRC script. Troj/Momma-B uses its own IRC client program so it can work on computers that do not have other IRC client software installed.

TROJ_SQLSPIDA.B: JS_SQLSPIDA.B uses this Trojan to scan the network for Internet Protocol (IP) addresses of SQL Servers via a Transmission Control Protocol (TCP) port 1433. It is Trend Micro's detection for the FSCAN tool that is renamed as SERVICES.EXE that is also downloadable from a legitimate Web site. It does not have a destructive payload.